PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-166029
(43)Date of publication of application : 10.06.2004

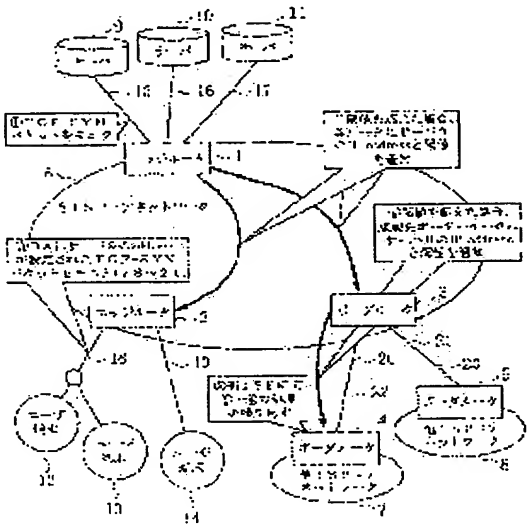
(51)Int.Cl. H04L 12/66
H04L 12/56

(21)Application number : 2002-330277
(22)Date of filing : 14.11.2002

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KANEKO HITOSHI
TOYOSHIMA AKIRA

(54) METHOD, SYSTEM AND PROGRAM FOR CONTROLLING DISTRIBUTED SERVICE REJECTION

(57)Abstract:
PROBLEM TO BE SOLVED: To minimize DDoS attack countermeasure processing in a network, to perform necessary processing, to provide a plan for obtaining an effect, to expand a processing range even to other ISPs and to apply accurate processing even to an attack packet that flows in from the other ISPs.
SOLUTION: Exit lines 15 to 17 on a server side of an edge router 1 in an ISP to which servers 9 to 11 to be a protection target, lines 18 and 19 on a user terminal side of each edge router 2 in a self-ISP 6 that houses user terminals 12 to 14, and lines 20 and 21 to other ISPs 7 and 8 of a border router 3 are selected. In processing at a normal time, a threshold for the maximum traffic of a TCP-SYN that can accept a server to be protected is set in advance to perform monitoring. When traffic exceeds the threshold, a part that exceeds the threshold is filtered, and the address of the server and the threshold are notified to all subscriber housing edges and all border routers in the same ISP.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号
特開2004-166029
(P2004-166029A)

(43)公開日 平成16年6月10日(2004.6.10)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	B	5K030
H04L 12/56	H04L 12/56	100Z	

審査請求 未請求 請求項の数 7 OL （全 12 頁）

(21)出願番号 特願2002-330277(P2002-330277)
(22)出願日 平成14年11月14日(2002.11.14)

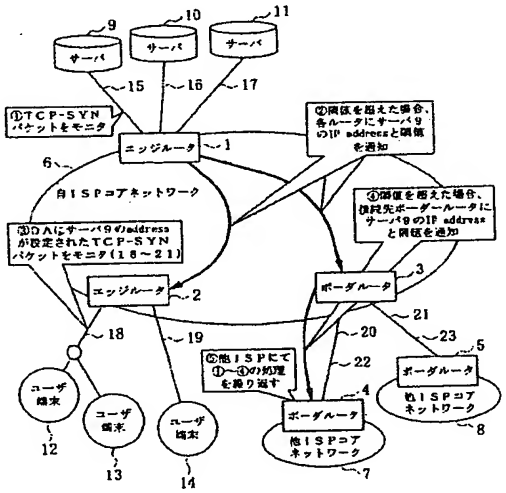
特許法第３０条第１項適用申請有り ２００２年８月２０日 社団法人電子情報通信学会発行の「電子情報通信学会２００２年ソサイエティ大会プログラム」に発表

(71)出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人 100077274
弁理士 磯村 雅俊
(74)代理人 100102587
弁理士 渡邉 昌幸
(72)発明者 金子 斉
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内
(72)発明者 豊島 鑑
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内

Fターム(参考) 5K030 GA15 HA08 HC01 HD03 HD06 LB05 LC15 MA04 MB09

(54)【発明の名称】分散型サービス拒絶防御方法およびシステム、ならびにそのプログラム

(57)【要約】
【課題】ネットワーク内のＤＤｏＳ攻撃対策処理を最小限に抑え、かつ必要な処理を行い、効果を得る方策を与え、かつ処理の範囲を他ＩＳＰにも拡張し、他ＩＳＰから流入する攻撃パケットについても的確な処理を行う。
【解決手段】保護対象となるサーバ９～１１が接続されるＩＳＰ内のエッジルータ１のサーバ側の出口回線１５～１７、ユーザ端末１２～１４を収容する自ＩＳＰ６内の各エッジルータ２のユーザ端末側の回線１８，１９、ボーダールータ３の他ＩＳＰ７，８への回線２０，２１を選択する。平常時の処理としては、予め保護するサーバが受け付けられるＴＣＰ－ＳＹＮの最大トラヒックの閾値を設定しておき、モニタを行う。トラヒックが当該閾値を越えた場合、超えた分のフィルタリングを行い、同一ＩＳＰ内の全加入者収容エッジおよび全ボーダールータへサーバのアドレスおよび当該閾値を通知する。



1

【特許請求の範囲】
【請求項１】
ＩＤＣ内のサーバマシンをＴＣＰ－ＳＹＮ－Ｆｌｏｏｄから保護するため、該ＩＤＣが接続されているＩＳＰ網のエッジルータは、該ＩＤＣ側の出口回線にて、該サーバマシンをｄｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓとするＴＣＰ－ＳＹＮパケットのトラヒックに対して閾値を設け、
該閾値を超えた場合に、超えた部分のトラヒックを廃棄し、
さらに、ユーザ端末を直接収容している各エッジルータおよびボーダールータに該閾値および該サーバマシンのａｄｄｒｅｓｓを通知し、
通知を受けた該エッジルータおよびボーダールータは、当該ＩＳＰとは反対側のインターフェースにて該閾値に基づくフィルタリングを行い、
さらに、該ボーダールータは、他ＩＳＰへのボーダールータに該閾値および該サーバマシンのａｄｄｒｅｓｓを通知し、
通知を受けた他ＩＳＰのボーダールータは、当該処理を繰り返し処理することを特徴とする分散型サービス拒絶防御方法。
【請求項２】
前記ＩＤＣが接続されているＩＳＰ網のエッジルータは、平常時の処理としては、予め保護するサーバが受け付けられるＴＣＰ－ＳＹＮの最大トラヒックの閾値を設定しておき、該閾値に基づいて単にモニタすることを特徴とする請求項１記載の分散型サービス拒絶防御方法。
【請求項３】
ＩＤＣ内のサーバマシンに接続され、保護の対象であるサーバマシンをｄｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓとするＴＣＰ－ＳＹＮパケットのトラヒックに対して、予め定めた閾値を超えた部分のトラヒックを廃棄する自ＩＳＰ網内のエッジルータと、
該エッジルータから前記閾値と前記サーバマシンのａｄｄｒｅｓｓ情報を受信して、前記ＩＳＰの反対側のインターフェースで該閾値に基づくフィルタリングを行う、ユーザ端末を収容するエッジルータまたはボーダールータと、
該ボーダールータから前記閾値と前記サーバマシンのａｄｄｒｅｓｓ情報を受信して、他ＩＳＰから自ＩＳＰの該ボーダールータ側のインターフェースで該閾値に基づくフィルタリングと前記各処理を行う他ＩＳＰ網内のボーダールータとを有することを特徴とする分散型サービス拒絶防御システム。
【請求項４】
自ＩＳＰ網内のエッジルータに、ＩＤＣ内の保護対象であるサーバマシンへの出口回線にて、該サーバマシンをｄｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓとするＴＣＰ－ＳＹＮパケットのトラヒックに対して閾値を設ける手順、該閾値を超えた場合に超えた部分のトラヒックを廃棄する手順、ユーザ端末を直接収容する各エッジルータおよびボーダルータに該閾値と該サーバマシンのａｄｄｒｅｓｓ情報を通知する手順を、実行させるためのプログラム。
【請求項５】
ユーザ端末を直接収容している自ＩＳＰ網内のエッジルータまたはボーダールータに、自ＩＳＰ網内の他エッジルータから閾値とａｄｄｒｅｓｓ情報を受信したことを確認する手順、当該ＩＳＰとは反対側のインターフェースにて該閾値に基づくフィルタリングを行う手順、直接収容している他ＩＳＰのボーダールータに対して該閾値とａｄｄｒｅｓｓ情報を通知する手順を、実行させるためのプログラム。
【請求項６】
他ＩＳＰ網内のボーダールータに、自ＩＳＰ網内のボーダールータから閾値とａｄｄｒｅｓｓ情報を受信したことを確認する手順、他ＩＳＰ網内のサーバマシンへの出口回線にて、該閾値に基づくフィルタリングを行う手段、他ＩＳＰ網内のユーザ端末を直接収容するエッジルータおよびボーダールータに対して、該閾値とａｄｄｒｅｓｓ情報を通知する手段を、実行させるためのプログラム。
【請求項７】
請求項４から請求項６のいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、ＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）網におけるＤＤｏＳ（Ｄｅｆｅａｔｉｎｇ　Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃に対するインターネットセキュリティ向上技術に関し、特にＤＤｏＳ攻撃に対する処理を最小限に止めることが可能な分散型サービス拒絶防御方法およびシステム、ならびにそのプログラムに関する。
【０００２】
【従来の技術】
従来のＤｏＳ（Ｄｅｎｉａｌ　ｏｆ　Ｓｅｒｖｉｃｅ）攻撃に対する文献としては、２００１年電子情報通信学会総合大会、Ｂ－７－１４の岡田浩一、外１名『ＤｏＳ攻撃のためのバックボーンネットワーク構築法』がある。ＤｏＳ攻撃には、それに使用されるパケットを形式から判断できるもの（形式不正型）と、形式からは判断できないが、送信元のアドレスが特定範囲に限定されるもの（アドレス限定型）と、送信元アドレスが特定範囲に限定されないもの（アドレス不定型）とがある。形式不正型に対しては、バッチ当て、あるいはパターンマッチングによるフィルタリングで対処が可能である。

3

【０００３】
また、アドレス限定型に対しては、ＩＤＳ（Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）による方法、つまり、特定範囲の送信元からのパケットの数が異常に多い場合、その範囲からのパケットの受信を制限または停止する対処法をとっている。アドレス不定型に対しては、上記文献により提案された方法、つまりイングレスフィルタリング装置を経由したパケットと、経由しないパケットを、パケットに安全性識別子を付加することで区別し、イングレスフィルタリング装置を経由したパケットを優先制御装置により優先してサーバに接続させる方法で対処する。
【０００４】
しかし、比較的単純なＤｏＳ攻撃については、一般的に攻撃力が弱く、比較的前より対策手法がとられていたが、ＤＤｏＳ（Ｄｉｓｔｒｉｂｕｔｅｄ　ＤｏＳ）に対しては、セキュリティ上脆弱な多数のＰＣを踏み台にして、一斉に攻撃を仕掛ける形態に進化しており、攻撃力は格段に増大している。
従来の方法では、ＴＣＰ－ＳＹＮ　Ｆｌｏｏｄの発見およびフィルタリング箇所として、保護対象のサーバが接続されるＩＳＰ内のエッジルータか、あるいは、加入者を収容するＩＳＰ内のエッジルータかのどちらか一方で、当該ＴＣＰ－ＳＹＮパケットのフィルタリングが行われるため、発見の精度が低かったり、発見してもフィルタリングが一律的なものとなってしまい、いわゆる正当な使用者も含めてフィルタリングされてしまうという問題があった。
ここで、ＴＣＰ－ＳＹＮ－Ｆｌｏｏｄとは、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）パケットのフィールドのＳＹＮの値にビットが立っているパケットを多量に送りつける攻撃のことである。
【０００５】
また、ネットワークレベルで処理を行う場合、常時、ネットワーク全体の各エッジルータでトラヒック情報を収集し、各ルーター間でトラヒック情報などを通知し合うなどして全ルータにてトラヒック情報を共有し、ＤＤｏＳ攻撃の発見およびフィルタリングなどの対処を行う方式もある。しかし、収集するトラヒック情報の対象によっては、各エッジルーターおよびネットワークの負荷が重いものになってしまい、あるいは、収集する情報の対象が狭い場合、発見の精度が落ちたり、また、フィルタリングの対象の絞り込みが不十分になったりする。また、ネットワークレベルで処理を行う場合でも、ＩＳＰ内に閉じた処理であったため、トラヒック量として相当な量を占めると思われる他ＩＳＰからボーダールータを通して流入してくるＴＣＰ－ＳＹＮ　Ｆｌｏｏｄに対しては、一律排除による手段を行うことになり、いわゆる正当なユーザのパケットも廃棄されてしまう。

4

【０００６】
【非特許文献１】
２００１年電子情報通信学会総合大会、Ｂ－７－１４の岡田浩一、外１名『ＤｏＳ攻撃のためのバックボーンネットワーク構築法』
【０００７】
【発明が解決しようとする課題】
前述のように、発見の精度、つまり攻撃が行われた場合には、即発見し、攻撃が行われなかった場合には、発見と位置付けない処理、および、フィルタリングの精度、つまり必要のない場合にはフィルタリングは行わず、攻撃者のパケットと正常ユーザのパケットを区別する処理、の精度を上げるためには、ネットワーク内の処理について、負荷が重い処理となり、平常時のサービスに影響を与えてしまう、という問題点があった。
【０００８】
本発明の目的は、このような問題点を解消し、ネットワーク内のＤＤｏＳ攻撃対策処理を最小限に抑え、かつ必要な処理を行い、効果を得る方策を与え、かつ処理の範囲を他ＩＳＰにも拡張し、他ＩＳＰから流入する攻撃パケットについても的確な処理ができるような分散型サービス拒絶防御方法およびシステム、ならびにそのプログラムを提供することにある。
【０００９】
【課題を解決するための手段】
本発明の分散型サービス拒絶防御方法は、まず、発見およびフィルタリングのポイントとして、保護対象となるサーバが接続されるＩＳＰ内のエッジルータのサーバ側の出口回線、加入者を収容する自ＩＳＰ内の各エッジルータの加入者側の回線、他ＩＳＰへの接続ポイントとなるボーダールータの他ＩＳＰへの回線を選択する。
平常時の処理としては、予め保護するサーバが受け付けられるＴＣＰ－ＳＹＮの最大トラヒックの閾値を設定しておき、モニタを行う。平常時の処理は、以上のみである。
【００１０】
トラヒックが当該閾値を越えた場合、超えた分のフィルタリングを行い、同一ＩＳＰ内の全加入者収容エッジおよび全ボーダールータへサーバのアドレスおよび当該閾値を通知する。
通知を受けた加入者収容エッジルータおよびボーダールータは、当該閾（および、加入者収容エッジルータではフィルタリングを行うインターフェース毎の収容ユーザ数）を基に、当該フィルタリングの閾値を決め、超えているものについてはフィルタリングを行う。加入者収容エッジルータでは、フィルタリング可能な加入者側の各レイヤのインターフェースにて、インターフェースに収容されている加入者の数が最小になるようなインターフェースを選択する。
【００１１】

5

各ボーダールータにおいて、トラヒックが閾値を超えてフィルタリングが行われた場合には、当該回線の接続先ＩＳＰのボーダールータにサーバのアドレスおよび閾値を通知する。通知を受けた他ＩＳＰでは、直接通知を受けたボーダールータを上記に記述したサーバ収容のエッジルータの位置付けとし、上記自ＩＳＰと同じ処理を行う。

【００１２】

【発明の実施の形態】

以下、図７～図１０により、ＤＤｏＳ攻撃対策を施さないネットワークでの説明を行い、その後、図１～図６によりＤＤｏＳ攻撃対策を施した本発明の処理について説明する。

図７は、本発明の機能（ＤＤｏＳ攻撃対策機能）を施さないネットワークの図である。

自ＩＳＰコアネットワーク６において、縁の部分に位置するエッジルータ１，２およびボーダールータ３が配置されている。７，８は、他ＩＳＰのコアネットワークであって、４，５は縁の部分に位置するボーダルータである。

９，１０，１１は、ＩＤＣ（Ｉｎｔｅｒｎｅｔ Ｄａｔａ Ｃｅｎｔｅｒ）内でｅコマース、コンテンツ配信などを行うサーバマシンであり、１２，１３，１４は自ＩＳＰに加入するユーザの端末である。１５～１７は、エッジルータ１におけるサーバ９～１１側のインターフェース、１８～１９はエッジルータ２におけるユーザ端末１２～１４側のインターフェース、２０～２１は、ボーダールータ３における他ＩＳＰのボーダールータ側のインターフェース、２２～２３は、それぞれ他ＩＳＰのボーダールータ４，５における自ＩＳＰボーダールータ側のインターフェースである。

【００１３】

図８は、ＩＰヘッダーおよびＴＣＰヘッダーのフィールドの図である。

ＴＣＰ－ＳＹＮパケットは、図８に示すように、Ｐｒｏｔｏｃｏｌは ＴＣＰを用い、ｆｌａｇｓ－ＳＹＮはそれぞれ１ビットのパケットである。そして、ＩＰｈｅａｄｅｒ、ＴＣＰ ｈｅａｄｅｒ、およびＤａｔａの順に送信される。ＴＣＰ ｈｅａｄｅｒ内のｆｌａｇｓフィールド６ビット（ビット８～１４）は、ＵＲＧ、ＡＣＫ、ＰＳＨ、ＲＳＴ、ＳＹＮ、ＦＩＮの６個の１ビットで構成される。

【００１４】

以下、用語の説明を行う。まず、攻撃者はセキュリティ上脆弱なユーザ端末に侵入し、攻撃用のソフトウェアを埋め込むなどの攻撃の準備をする。図７では、進入されたユーザ端末を１２および１３、進入されなかったユーザ端末を１４とする。また、ユーザ端末１２，１３のように、攻撃者に乗っ取られたユーザ端末を、以降は『ゾンビ』と呼ぶ。

6

【００１５】

攻撃者は、乗っ取ったユーザ端末（図１の１２，１３）に対して、攻撃対象となるサーバ（図１の９）に対して一斉に多量のＴＣＰ－ＳＹＮパケットを送信するよう命令する。このとき、ＴＣＰ－ＳＹＮパケットのｓｏｕｒｃｅ ａｄｄｒｅｓｓ（送信元アドレス）にはランダム値が設定される。

一方、各攻撃端末よりの多量のＴＣＰ－ＳＹＮパケットを受け取ったサーバ９は、それぞれ１つずつのパケット毎にコネクションの処理に移る。この処理を、３ｗａｙ－ｈａｎｄ－ｓｈａｋｅと呼ぶ。

【００１６】

図９は、正常な３ｗａｙ－ｈａｎｄ－ｓｈａｋｅのシーケンスチャートである。

３ｗａｙ－ｈａｎｄ－ｓｈａｋｅは、ユーザ端末１２，１３からサーバ９へ、ＴＣＰ－ＳＹＮパケット（３１）を送付する。ＴＣＰ－ＳＹＮパケット（３１）がサーバ９に送付されると、これを受信したサーバ９はパケットのｓｏｕｒｃｅ ａｄｄｒｅｓｓ先にＴＣＰ－ＡＣＫ＋ＳＹＮパケット（３２）を返送する。

ｓｏｕｒｃｅ ａｄｄｒｅｓｓに正しい値（１２，１３のＩＰ ａｄｄｒｅｓｓ）が設定されていれば、当該パケットはユーザ端末１２，１３にたどり着き、当該パケットを受け取ったユーザ端末１２，１３は再度、ＴＣＰ－ＡＣＫパケット（３３）をサーバ９に返送し、これにてＴＣＰコネクションが確立する（３４）。

【００１７】

しかし、通常ゾンビ１２，１３は、サーバ９にＴＣＰ－ＳＹＮパケットを送付する際に、ｓｏｕｒｃｅ ａｄｄｒｅｓｓにランダム値を設定して送付するため、サーバ９は、そのランダム値のＩＰ ａｄｄｒｅｓｓへＴＣＰ－ＡＣＫ＋ＳＹＮパケットを送付するため、当該パケットはゾンビ１２，１３にたどり着かない。

【００１８】

図１０は、ゾンビ１２，１３がサーバ９にＴＣＰ－ＳＹＮパケットを送付する場合のシーケンスチャートである。

ゾンビ１２，１３からＴＣＰ－ＳＹＮパケット（４１）をサーバ９に送信する場合、ゾンビ１２，１３では、ｓｏｕｒｃｅ ａｄｄｒｅｓｓにランダム値が設定されて送付されるので、サーバ９からＴＣＰ－ＡＣＫ＋ＳＹＮパケット（４２）を返送する場合、ユーザ端末１２，１３とは別アドレスに送付されてしまう。従って、ユーザ端末１２，１３にはＴＣＰ－ＡＣＫ＋ＳＹＮパケット（４２）は届かない。その結果、サーバ９にも、ＴＣＰ－ＡＣＫパケット（４３）は届かないことになる。従って、サーバ９は、タイムアウトするまでＴＣＰ－ＡＣＫパケット（４３）の待ち状態となる。従って、多数のゾンビより当該多量のＴＣＰ－ＡＣＫパケットが送られる

ため、サーバ９は多数の待ち状態を維持することになり、リソース不足などにより機能停止してしまう。

【００１９】

（実施例）

以下、本発明の実施例について説明する。

図１は、ＤＤｏＳ攻撃対策を施した本発明の実施例を示すネットワーク図である。また、図３は、本発明のエッジルータにおけるフィルタリングのルール設定画面の例を示す図である。

ここでは、保護対象のサーバをサーバ９とする。先ず、エッジルータ１におけるフィルタリングのルール設定を図３のように行う。エッジルータ１は、インターフェース１５にてサーバ９のＩＰ　ａｄｄｒｅｓｓをｄｅｓｔｉｎａｔｉｏｎａｄｄｒｅｓｓに（５３，５４）、ＰＲＯＴＯＣＯＬをＴＣＰに（５５）ＣＯＮＴＲＯＬ　ＦＬＡＧＳをＳＹＳに（５６）、一定の閾値を設け、閾値をオーバーする部分につきフィルタリングを行う。すなわち、ＤＤｏＳ攻撃が行われても、トラヒック値が閾値の範囲内であれば、エッジルータ１は何の処理も行わない。

【００２０】

閾値としては、予め当該サーバ９が正常運用可能なトラヒック値を設定しておく（５７）。ここでは、予め６０Ｋｂｐｓが設定されている。

また、トラヒックが閾値を超えた際に通知するルータのＩＰ　ａｄｄｒｅｓｓも予め設定しておく（５８）。通知先のルータについては、自ルータ以外の自ＩＳＰコアネットワーク６内の全てのエッジルータおよびボーダールータのＩＰ　ａｄｄｒｅｓｓを設定しておく。ここでは、１１１．１１．２２．３と２２．２２．３３．４が設定されている。

エッジルータ１は、トラヒック量が当該閾値を超えたとき、通知先に記してあるルータへ、当該閾値情報およびサーバ９のＩＰ　ａｄｄｒｅｓｓ情報を添付して通知を行う。

【００２１】

図４，図５は、エッジルータ２およびボーダールータ３におけるフィルタリングルールの設定画面の例を示す図である。

図４において、通知を受けた各エッジルータおよびボーダールータ（図１の２，３）は、インターフェース１８～２１において送付されたＩＰ　ａｄｄｒｅｓｓをＤＥＳＴＩＮＡＴＩＯＮ　ＡＤＤＲＥＳＳに（６３）、ＰＲＯＴＯＣＯＬをＴＣＰに（６５）、ＣＯＮＴＲＯＬ　ＦＬＡＧＳをＳＹＮに（６６）、閾値を設け（６７）、閾値をオーバーする部分についてフィルタリングを行う。このとき、エッジルータの対象となるインターフェースとしては、ユーザ端末に対してフィルタリング可能な、なるべく細かいインターフェースを選択する。図４では、ＶＩＲＴＵＡＬ　ＲＯＵＴＥＲの場合を例としている（図１の１８）。図４の場合には、閾値を超えた場合にも、通知しない（６８）ことに設定されている。なお、閾値としては、通知閾値／１０００が設定されている。

【００２２】

図５においても、図４と同じように、インターフェース１８～２１において送付されたＩＰ　ａｄｄｒｅｓｓをＤＥＳＴＩＮＡＴＩＯＮ　ＡＤＤＲＥＳＳに（７３）、ＰＲＯＴＯＣＯＬをＴＣＰに（７５）、ＣＯＮＴＲＯＬ　ＦＬＡＧＳをＳＹＮに（７６）、閾値を設け（７７）、閾値をオーバーする部分についてフィルタリングを行う。このとき、エッジルータの対象となるインターフェースとしては、ユーザ端末に対してフィルタリング可能な、なるべく細かいインターフェースを選択する。図５では、ＶＩＲＴＵＡＬ　ＲＯＵＴＥＲの場合を例としている（図１の２０）。閾値については、予め、通知された閾値と当該インターフェースに収容されるユーザ端末数を基にした計算式を記しておく（７７）。ここでは、通知閾値／５が設定されている。

【００２３】

当該マシンがボーダールータの場合には、トラヒックが閾値を超えた場合の通知先ＩＰ　ＡＤＤＲＥＳＳを記す（７８）。通知先ＩＰ　ＡＤＤＲＥＳＳには、当該インターフェースの接続先の他ＩＳＰコアネットワークのボーダールータ（図１の４，５）のアドレスを記しておく。

ボーダールータは、ルールの記述に従って、トラヒックが閾値を超えた場合に接続先他ＩＳＰのボーダールータに通知を行う。通知を受けたボーダールータ４，５は、本処理の最初にエッジルータ１がインターフェース１５を監視したのと同様に、それぞれインターフェース２２，２３を監視し、他ＩＳＰコアネットワーク内にて上記自ＩＳＰと同様の処理を繰り返す。

【００２４】

図６は、他ＩＳＰのボーダールータにおけるフィルタリングのルール設定画面の例を示す図である。

図６の設定画面が、他と異なる点は、当該ボーダールータにて設定するルールにて、ＳＯＵＲＣＥ　ＡＤＤＲＥＳＳは通知されたＩＰ　ａｄｄｒｅｓｓを用い、閾値は、通知された閾値を使用する点である。

すなわち、インターフェース１８～２１において送付されたＩＰ　ａｄｄｒｅｓｓをＤＥＳＴＩＮＡＴＩＯＮ　ＡＤＤＲＥＳＳに（８３）、ＰＲＯＴＯＣＯＬをＴＣＰに（８５）、ＣＯＮＴＲＯＬ　ＦＬＡＧＳをＳＹＮに（８６）、閾値は通知された閾値（通知閾値）とし（８７）、閾値をオーバーする部分についてフィルタリングを行う。図６でも、ＶＩＲＴＵＡＬ　ＲＯＵＴＥＲの場合を例としている（図１の２２）。図６の場合、通知先ＩＰ　ＡＤＤＲＥＳＳには、当該インターフェースの接続先の他ＩＳＰコアネットワークのボーダールータ（図

１の４，５）のアドレスを記しておく（８８）。

【００２５】

図１に戻り、本発明の処理を説明する。

▲１▼エッジルータ１では、図３に示すルール設定画面により、インターフェース１５でパケットのトラヒックが閾値を超えるか否かを監視（モニタ）する。

▲２▼閾値を超えた場合には、各ルータ（エッジルータ２、ボーダールータ３）にサーバ９のＩＰ　ａｄｄｒｅｓｓと閾値を通知する。

▲３▼エッジルータ２では、図４，図５に示すルール設定画面により、ＤＡにサーバ９のａｄｄｒｅｓｓが設定されたＴＣＰ－ＳＹＮパケットをインターフェース１８～２１でモニタ、すなわち、閾値を超えたか否かを監視する。

▲４▼閾値を超えた場合には、接続先ボーダールータにサーバ９のＩＰ　ａｄｄｒｅｓｓと閾値を通知する。

▲５▼他ＩＳＰのボーダールータ４，５では、図６に示すルール設定画面により、上記▲１▼～▲４▼の処理を繰り返し行う。

【００２６】

図２は、本発明の一実施例を示す分散型サービス拒絶防御方法の動作フローチャートである。

先ず、エッジルータ１は、インターフェース１５でＤｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓがサーバ９のＩＰ　ａｄｄｒｅｓｓ、ｐｒｏｔｏｃｏｌの値がＴＣＰ、Ｆｌａｇｓの値がＳＹＮであるパケットのトラヒックが閾値を越えるか否かを監視する（ステップ１０１）。

トラヒックが閾値を超えたならば（ステップ１０２）、超えた部分につき、パケットをフィルタリングする（ステップ１０３）。同一ＩＳＰ内の各エッジルータに閾値、サーバ９のＩＰアドレスを通知する（ステップ１０４）。

【００２７】

次に、エッジルータ２およびボーダールータ３のインターフェース１８～２１でＤｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓの値がサーバ９のＩＰ　ａｄｄｒｅｓｓ、ｐｒｏｔｏｃｏｌの値がＴＣＰ、ｆｌａｇｓの値がＳＹＮであるパケットのトラヒックが閾値（通知された閾値より計算）を超えるか否かを監視する（ステップ１０５）。

トラヒックが閾値を超えたならば（ステップ１０６）、超えた部分につき、パケットをフィルタリングする（ステップ１０７）。そして、自エッジルータの種類を判別し（ステップ１０８）、加入者収容エッジルータであれば、処理を終了し、ボーダールータであれば、他ＩＳＰボーダールータ（インターフェース２０，２１の接続先）に閾値、サーバ９のＩＰアドレスを通知する（ステップ１０９）。

【００２８】

次に、他ＩＳＰのボーダールータ４，５は、自ＩＳＰコアネットワーク６にインターフェース１５を、インターフェース２２，２３に置き換えて、ステップ１０１～１０８の処理を実行する（ステップ１１０）。すなわち、ボーダールータ４，５は、インターフェース２２，２３でＤｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓがサーバ９のＩＰａｄｄｒｅｓｓ、ｐｒｏｔｏｃｏｌの値がＴＣＰ、Ｆｌａｇｓの値がＳＹＮであるパケットのトラヒックが通知された閾値を超えるか否かを監視し（ステップ１０１）、トラヒックが閾値を超えたならば（ステップ１０２）、超えた部分につきパケットをフィルタリングし（ステップ１０３）、同一ＩＳＰ内の各エッジルータおよびボーダールータに閾値、サーバ９のＩＰアドレスを通知する（ステップ１０４）。なお、図１には、記載が省略されているが、他ＩＳＰコアネットワーク７，８にも、ユーザ端末が収容されるエッジルータが配置されている。また、ステップ１１０では、他ＩＳＰのコアネットワーク７，８内に別のボーダールータがある限り、先へ先へと芋づる式に処理されることになる。この場合の全てのボーダールータは、図６に示すように、通知されたアドレス、閾値を利用する。

【００２９】

他ＩＳＰのエッジルータおよびボーダールータのインターフェースでＤｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓの値がサーバ９のＩＰ　ａｄｄｒｅｓｓ、ｐｒｏｔｏｃｏｌの値がＴＣＰ、ｆｌａｇｓの値がＳＹＮであるパケットのトラヒックが通知された閾値を超えるか否かを監視し（ステップ１０５）、トラヒックが閾値を超えたならば（ステップ１０６）、超えた部分につき、パケットをフィルタリングし（ステップ１０７）、自エッジルータの種類を判別し（ステップ１０８）、加入者収容エッジルータのときは処理を終了し、ボーダールータのときには、他ＩＳＰボーダールータに閾値、サーバ９のＩＰアドレスを通知する（ステップ１０９）。

【００３０】

なお、図２のフローにおいて、ステップ１０１～１０４は自ＩＳＰコアネットワークのエッジルータ１が実行すべきプログラムに変換することができ、ステップ１０５～１０９は自ＩＳＰコアネットワークのエッジルータ２およびボーダールータ３が実行すべきプログラムに変換することができ、ステップ１１０（ステップ１０１～１０９）は他ＩＳＰコアネットワークのボーダールータ４，５が実行すべきプログラムに変換することができる。

そして、これらのプログラムをＣＤ－ＲＰＭなどの記録媒体に格納しておけば、それを携帯してＩＳＰコアネットワークのエッジルータまたはボーダールータに装着することで、コンピュータにプログラムをインストールし、実行させることにより、本発明を容易に実現させることができる。

【００３１】

【発明の効果】
以上説明したように、本発明によれば、ＤＤｏＳ攻撃に対する処理を最小限に止めることができる。すなわち、平常時には、エッジルータ１のみにて、サーバ９へのトラヒックを監視するのみである。ＤＤｏＳ攻撃が行われても、攻撃のトラヒックが限界値に達するまでは処理は行われない。攻撃のトラヒックが限界値を超えた場合でも、同一ＩＳＰ内のエッジルータへの通知情報は極く少なく、ネットワーク負荷への影響も殆んどない。

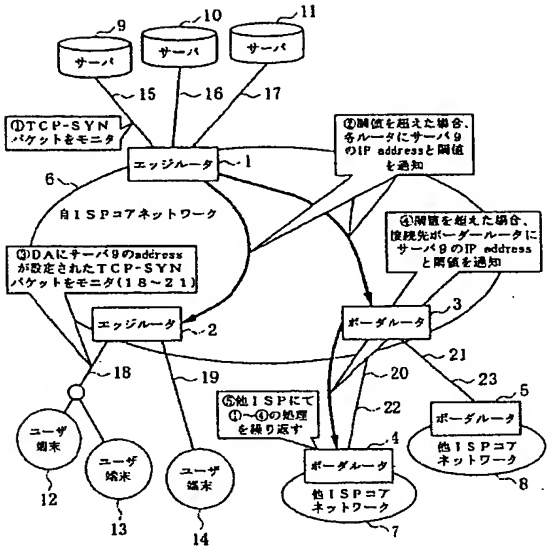
【００３２】
また、モニタ、フィルタリングがエッジルータ１とエッジルータ２、ボーダールータ３で２段階で実施されるため、エッジルータ２、ボーダールータ３のみで実施されるよりも発見の精度を高められ、処理の精度を高めることができる。
また、エッジルータ２、ボーダールータ３でのフィルタリング処理の閾値も高目に設定でき、正当ユーザへの影響を最小限に止めることができる。
フィルタリング処理をエッジルータ２、ボーダールータ３におけるフィルタリング処理を、自ＩＳＰコアネットワーク１と反対側の各インターフェース毎に行うため、攻撃者の絞り込みをすることができ、正当ユーザへの影響を最小限にすることができる。

【００３３】
ボーダールータ間の通知を行うことにより、単に自ＩＳＰコアネットワークのボーダールータ３のみでフィルタリングを行う場合と比べて、接続先の他ＩＳＰ７，８でも同様の処理が繰り返されることにより、攻撃元を更に絞り込むことができ、他ＩＳＰの正当ユーザも救済することができる。

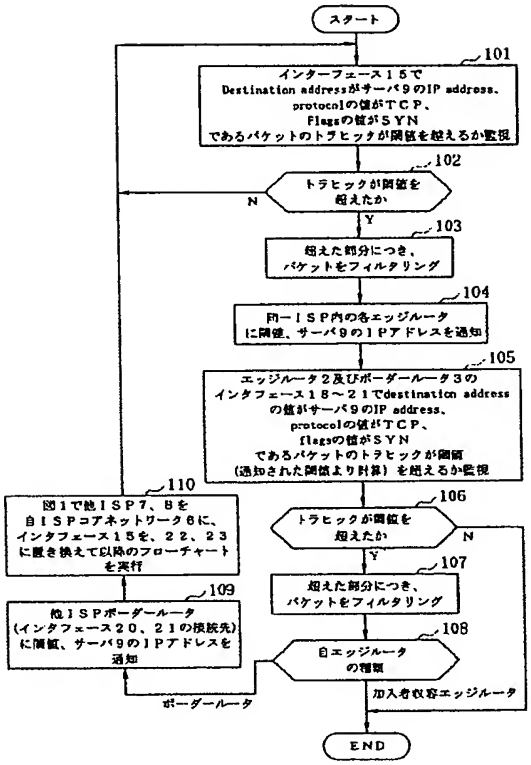
【図面の簡単な説明】
【図１】本発明の一実施例を示す分散型サービス拒絶防御装置のネットワーク図である。
【図２】図１における分散型サービス拒絶防御方法の動作フローチャートである。
【図３】図１におけるエッジルータ１のルール設定画面の例を示す図である。
【図４】図１におけるエッジルータ２のルール設定画面の例を示す図である。
【図５】図１におけるボーダールータ３のルール設定画面の例を示す図である。
【図６】図１におけるボーダールータ４でのルール設定画面の例を示す図である。
【図７】ＤＤｏＳ攻撃対策を施さないネットワークを示す図である。
【図８】ＩＰヘッダ、ＴＣＰヘッダのフォーマットを示す図である。
【図９】正常なＴＣＰコネクション処理（３ウェイハンドシェイク処理）のシーケンスチャートである。
【図１０】ＴＣＰ－ＳＹＮ　Ｆｌｏｏｄが行われた場合のシーケンスチャートである。

【符号の説明】
１…サーバを収容する自ＩＳＰのエッジルータ、
２…加入者を収容する自ＩＳＰのエッジルータ、
３…他ＩＳＰと接続するボーダールータ、
４～５…他ＩＳＰとの接続における他ＩＳＰ側のボーダールータ、
６…自ＩＳＰコアネットワーク、７～８…他ＩＳＰコアネットワーク、
９～１１…自ＩＳＰにてエッジルータ１に収容されるサーバ、
１２～１４…自ＩＳＰにてエッジルータ２に収容されるユーザ端末、
１５～１７…エッジルータ１におけるサーバ９～１１側のインターフェース、
１８～１９…エッジルータ２のユーザ端末１２～１４のインターフェース、
２０～２１…ボーダールータ３の他ＩＳＰボーダルータ側インターフェース、
２２～２３…他ＩＳＰボーダールータの自ボーダルータ側インタフェース。

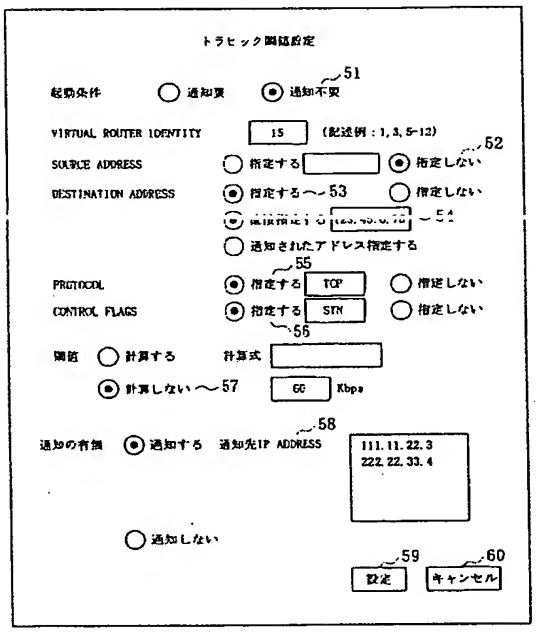
【図１】


サーバ
サーバ
サーバ
9
10
11
15
16
17
①TCP-SYN パケットをモニタ
エッジルータ
1
②閾値を超えた場合、各ルータにサーバ９のIP addressと閾値を通知
6
自ＩＳＰコアネットワーク
④閾値を超えた場合、後続先ボーダールータにサーバ９のIP addressと閾値を通知
③DAにサーバ９のaddressが設定されたTCP-SYNパケットをモニタ(１８～２１)
エッジルータ
2
ボーダルータ
3
21
18
19
20
23
5
⑤他ＩＳＰにて①～④の処理を繰り返す
22
ボーダルータ
4
他ＩＳＰコアネットワーク
8
他ＩＳＰコアネットワーク
7
ユーザ端末
ユーザ端末
ユーザ端末
12
13
14

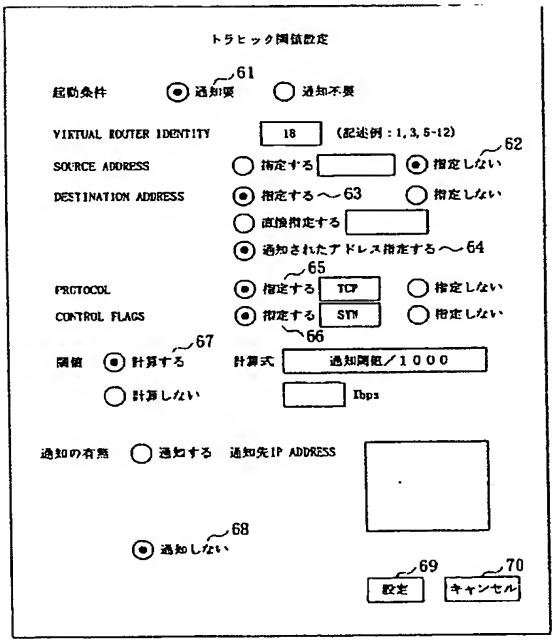
【図２】


スタート
101
インターフェース１５で Destination addressがサーバ９のIP address、protocolの値がＴＣＰ、Flagsの値がＳＹＮであるパケットのトラヒックが閾値を超えるか監視
102
トラヒックが閾値を超えたか
N
Y
103
超えた部分につき、パケットをフィルタリング
104
同一ＩＳＰ内の各エッジルータに閾値、サーバ９のＩＰアドレスを通知
105
エッジルータ２及びボーダールータ３のインタフェース１８～２１でdestination addressの値がサーバ９のIP address、protocolの値がＴＣＰ、flagsの値がＳＹＮであるパケットのトラヒックが閾値（通知された閾値より計算）を超えるか監視
106
トラヒックが閾値を超えたか
N
Y
107
超えた部分につき、パケットをフィルタリング
108
自エッジルータの種類
ボーダールータ
加入者収容エッジルータ
110
図１で他ＩＳＰ７、８を自ＩＳＰコアネットワーク６に、インタフェース１５を、２２、２３に置き換えて以降のフローチャートを実行
109
他ＩＳＰボーダールータ（インタフェース２０、２１の根拠先）に閾値、サーバ９のＩＰアドレスを通知
END

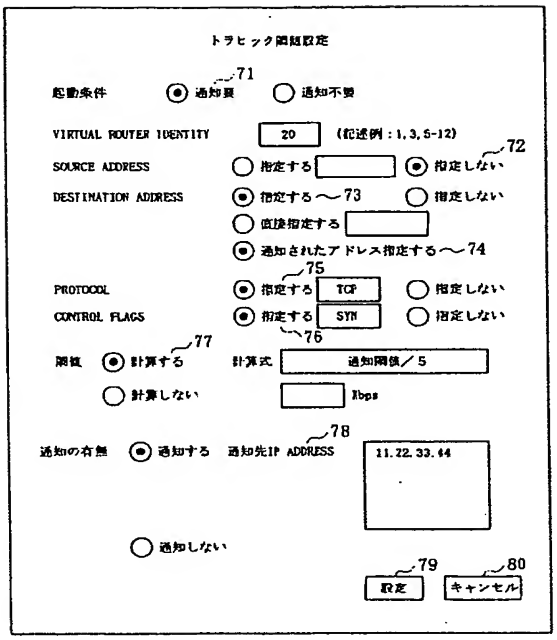
【図３】


トラヒック閾値設定
起動条件
通知要
通知不要
51
VIRTUAL ROUTER IDENTITY
15
(記述例：1,3,5-12)
SOURCE ADDRESS
指定する
指定しない
52
DESTINATION ADDRESS
指定する
53
指定しない
54
通知されたアドレス指定する
PROTOCOL
55
指定する
TCP
指定しない
CONTROL FLAGS
指定する
SYN
指定しない
56
閾値
計算する
計算式
計算しない
57
60
Kbps
通知の有無
通知する
通知先IP ADDRESS
58
111.11.22.3
222.22.33.4
通知しない
59
設定
キャンセル
60

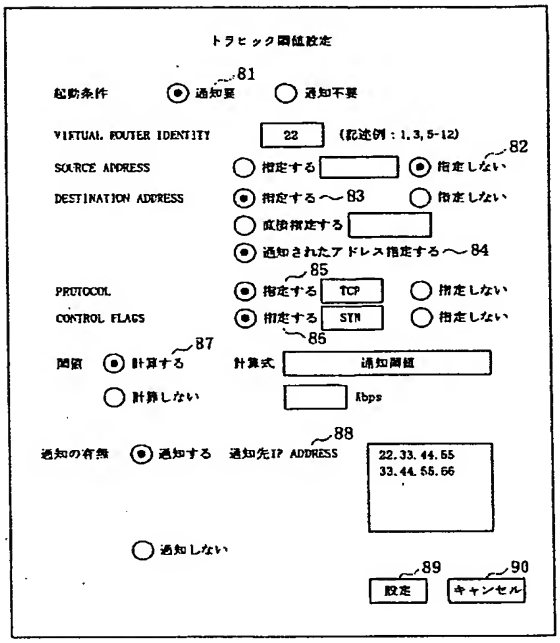
【図４】


トラヒック閾値設定
起動条件
通知要
通知不要
61
VIRTUAL ROUTER IDENTITY
18
(記述例：1,3,5-12)
SOURCE ADDRESS
指定する
指定しない
62
DESTINATION ADDRESS
指定する
63
指定しない
直接指定する
通知されたアドレス指定する
64
PROTOCOL
65
指定する
TCP
指定しない
CONTROL FLAGS
指定する
SYN
指定しない
66
閾値
計算する
67
計算式
通知閾値／１０００
計算しない
Ibps
通知の有無
通知する
通知先IP ADDRESS
通知しない
68
69
設定
キャンセル
70

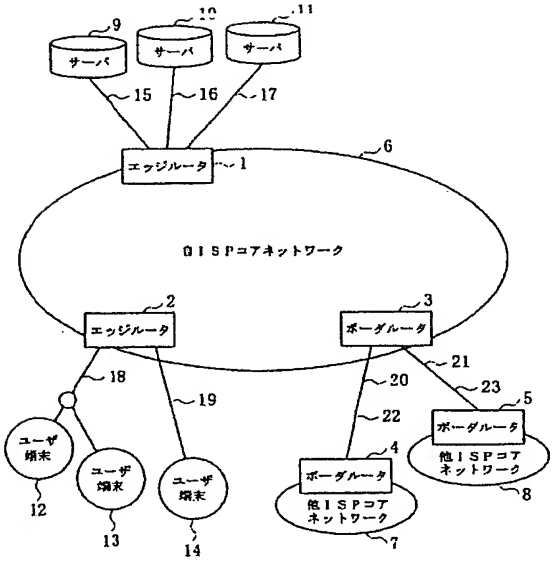
【図５】



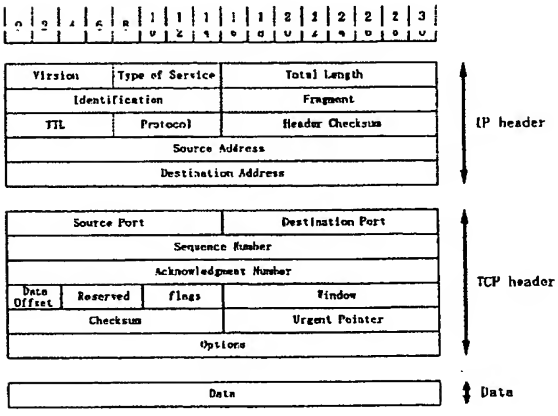
【図６】



【図７】

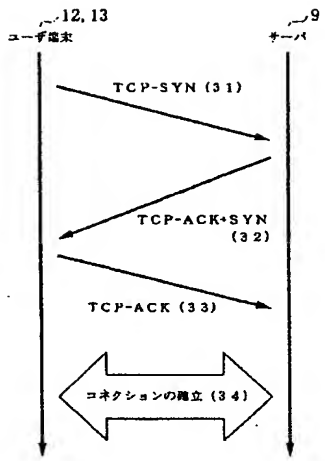


【図８】

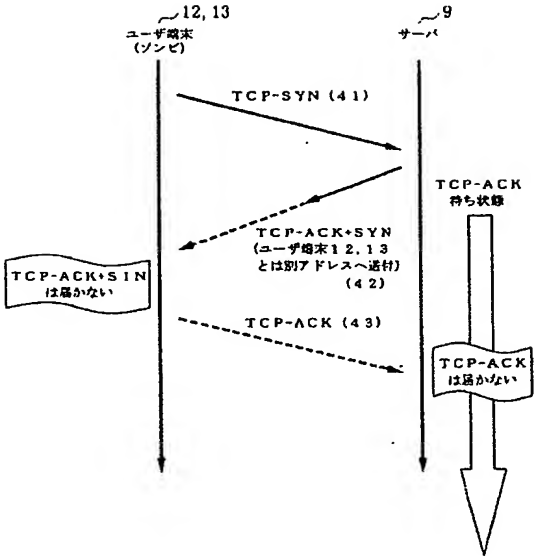


※ flagsフィールド6bitは、それぞれ、６つの１bitフィールド URG, ACK, PSH, RST, SYN, FINで構成される。

【図９】


12, 13
ユーザ端末
9
サーバ
TCP-SYN (31)
TCP-ACK+SYN
(32)
TCP-ACK (33)
コネクションの確立 (34)

【図１０】


12, 13
ユーザ端末
(ゾンビ)
9
サーバ
TCP-SYN (41)
TCP-ACK
待ち状態
TCP-ACK+SYN
(ユーザ端末12, 13
とは別アドレスへ送付)
(42)
TCP-ACK+SYN
は届かない
TCP-ACK (43)
TCP-ACK
は届かない